

CHESTNUT CAMBRONNE PA

Bryan L. Bleichner (CAL BAR # 220340)
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Phone: (612) 339-7300
Email: *bbleichner@chesnutcambronne.com*

**UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA**

Blake Mijangos, individually and on behalf
of all others similarly situated,

Plaintiff,

v.

Form I-9 Compliance LLC,

Defendant.

Hon. Judge _____
Case No.: 8:24-cv-1210

CLASS ACTION

**COMPLAINT FOR DAMAGES,
INJUNCTIVE AND EQUITABLE
RELIEF FOR:**

- 1. NEGLIGENCE;**
- 2. INVASION OF PRIVACY;**
- 3. UNJUST ENRICHMENT;**
- 4. BREACH OF IMPLIED
CONTRACT;**
- 5. CALIFORNIA'S UNFAIR
COMPETITION LAW
("UCL") § 17200 –
UNLAWFUL BUSINESS
PRACTICE;**
- 6. CALIFORNIA UCL § 17200 –
UNFAIR BUSINESS
PRACTICE;**
- 7. BREACH OF CALIFORNIA
SECURITY NOTIFICATION
LAWS CIVIL CODE § 1798.82**

DEMAND FOR JURY TRIAL

1 Plaintiff Blake Mijangos (“Plaintiff”) brings this Class Action Complaint
2 against Form I-9 Compliance, LLC (“Defendant” or “Form I-9”), in his individual
3 capacity and on behalf of all others similarly situated, and alleges, upon personal
4 knowledge as to own actions and his counsel’s investigations, and upon information
5 and belief as to all other matters, as follows:
6

7 **INTRODUCTION**

8
9 1. This class action arises out of the recent targeted cyberattack and data
10 breach in February 2024 (“Data Breach”) on Defendant’s network that resulted in
11 unauthorized access to its members’ sensitive personal data. As a result of the Data
12 Breach, Plaintiff and over 27,000 Class Members had their most sensitive personal
13 information accessed, exfiltrated, and stolen, causing them to suffer ascertainable
14 losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses
15 and the value of their time reasonably incurred to remedy or mitigate the effects of
16 the attack.
17
18

19 2. Information compromised in the Data Breach includes individuals’
20 Private Identifiable Information (“PII” or “Private Information”) which includes,
21 names, address, Social Security number, date of birth and employment “hire date”.
22
23

24 3. Plaintiff brings this class action lawsuit on behalf of himself and those
25 similarly situated to address Defendant’s inadequate safeguarding of Plaintiff’s and
26 Class Members’ Private Information that it collected and maintained.
27

1 4. Defendant maintained the Private Information in a reckless and
2 negligent manner. In particular, the Private Information was maintained on
3 Defendant's computer system and network in a condition vulnerable to cyberattacks.
4
5 Upon information and belief, the mechanism of the cyberattack and potential for
6 improper disclosure of Plaintiff's and Class Members' Private Information was a
7 known risk to Defendant, and thus Defendant was on notice that failing to take steps
8 necessary to secure the Private Information from those risks left that property in a
9 dangerous condition.
10

11 5. Plaintiff's and Class Members' identities are now at risk because of
12 Defendant's negligent conduct because the Private Information that Defendant
13 collected and maintained was exposed and is now in the hands of data thieves.
14

15 6. Armed with the Private Information accessed in the Data Breach, data
16 thieves can commit a variety of crimes including, e.g., opening new financial
17 accounts in Class Members' names, taking out loans in Class Members' names,
18 using Class Members' names to obtain medical services, obtaining driver's licenses
19 and passports in Class Members' names but with another person's photograph, and
20 giving false information to police during an arrest.
21
22

23 7. As a result of the Data Breach, Plaintiff and Class Members have been
24 exposed to a heightened and imminent risk of financial fraud and identity theft.
25
26
27

1 Plaintiff and Class Members must now and in the future closely monitor their
2 financial accounts to guard against identity theft.

3 8. Plaintiff and Class Members may also incur out of pocket costs for, e.g.,
4 purchasing credit monitoring services, credit freezes, credit reports, or other
5 protective measures to deter and detect identity theft.
6

7 9. Through his Complaint, Plaintiff seeks to remedy these harms on behalf
8 of himself and all similarly situated individuals whose Private Information was
9 accessed during the Data Breach.
10

11 10. Plaintiff seeks remedies including, but not limited to, compensatory
12 damages, statutory damages, reimbursement of out-of-pocket costs, and injunctive
13 relief including improvements to Defendant's data security systems, future annual
14 audits, and adequate credit monitoring services funded by Defendant.
15
16

17 11. Accordingly, Plaintiff brings this action against Defendant seeking
18 redress for its unlawful conduct and asserting claims on behalf of the Class (defined
19 *infra*) for negligence, invasion of privacy, unjust enrichment, breach of implied
20 contract, unlawful business practice, unfair business practice, and Breach of
21 California Security Notification Laws Civil Code § 1798.82.
22
23

24 **PARTIES**

25 ***Plaintiff Blake Mijangos***

26 12. Plaintiff received consulting services through Defendant and Plaintiff
27

1 received a letter from Defendant dated May 31, 2024, on or about that date (the
2 “Notice of Data Breach Letter”). The Notice of Data Breach Letter notified Plaintiff
3 that “on April 12, 2024, [Defendant] identified unusual activity on its
4 network...[Defendant] has evidence that an unauthorized party accessed or took
5 certain information from [Defendant’s] network on February 5, 2024.”
6

7 13. The Notice of Data Breach Letter informed Plaintiff Blake Mijangos
8 that an unauthorized party accessed Plaintiff’s Private Information, including
9 personal information and his Social Security number.
10

11 ***Defendant Form I-9 Compliance (“Form I-9”)***
12

13 14. Defendant is a compliance consulting company in Southern California
14 that acquired, utilized, and stored Plaintiff’s and Class Member’s Private
15 Information.
16

17 15. Upon information and belief, Defendant is headquartered in Newport
18 Beach, Orange County, State of California.
19

20 16. Moreover, Defendant’s website specifies that it is located in Newport
21 Beach, Orange County, California.
22

23 **JURISDICTION AND VENUE**
24

25 17. This Court has subject matter and diversity jurisdiction over this action
26 under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of
27 controversy exceeds the sum or value of \$5 million, exclusive of interest and costs,
28

1 there are more than 100 members in the proposed Class, and at least one Class
2 Member is a citizen of a state different from Defendant to establish minimal
3 diversity.
4

5 18. This court has personal jurisdiction over Defendant named in this action
6 because Defendant is headquartered in this District and conducts substantial business
7 in this District.
8

9 19. Venue is proper in this District under 28 U.S.C. §1391(b) because
10 Defendant is headquartered in this District and a substantial part of the events or
11 omissions giving rise to Plaintiff's claims occurred in this District.
12

13 **ALLEGATIONS**

14 ***Defendant's Business***

15 20. Defendant is a Limited Liability Company, with its principal place of
16 business in Newport Beach, California.
17

18 21. Defendant began operations as a consulting services business in 2004
19 and is currently serving over 1,000 employers across the United States.¹
20

21 22. Form I-9 Compliance offers tech solutions and consulting services for
22 Form I-9 and E-Verify compliance, including electronic Form I-9 processing, and
23 automated right-to-work verifications.²
24

25
26 ¹ See <https://www.linkedin.com/company/formi9/about/> (last accessed June 4, 2024).

27 ² See <https://www.formi9.com/about-us/> (last accessed June 4, 2024).
28

23. On information and belief, in the ordinary course of business as a condition of service, Defendant required members, including Plaintiff, to provide copious amounts of sensitive personal and private information, such as the Private Information compromised in the Data Breach.

The Cyberattack & Data Breach

24. On or about April 12, 2024, Defendant identified unusual activity on its network.

25. Defendant immediately began an investigation with the assistance of cybersecurity specialists to determine there is evidence that an unauthorized party accessed or took certain information from Defendant's network on or about February 5, 2024.

26. Defendant had obligations created by contract, industry standards, common law, and its own promises and representations made to Plaintiff and Class Members that it would keep their Private Information confidential and protect it from unauthorized access and disclosure.

27. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

1 ***Defendant Knew the Private Information on its Network was a Target***

2 28. In light of recent high-profile data breaches at other companies in the
3 consulting industry, Defendant knew or should have known that their electronic
4 records would be targeted by cybercriminals.
5

6 29. Cyberattacks have become so notorious that the FBI and U.S. Secret
7 Service have issued a warning to potential targets, so they are aware of, and prepared
8 for, a potential attack. As one report explained, “[e]ntities like smaller municipalities
9 and hospitals are attractive. . . because they often have lesser IT defenses and a high
10 incentive to regain access to their data quickly.”³
11
12

13 30. Therefore, the increase in such attacks, and attendant risk of future
14 attacks, was widely known to the public and to anyone in Defendant’s industry,
15 including Defendant.
16

17 ***Defendant Failed to Comply with FTC Guidelines***

18 31. The Federal Trade Commission (“FTC”) has promulgated numerous
19 guides for businesses which highlight the importance of implementing reasonable
20 data security practices. According to the FTC, the need for data security should be
21 factored into all business decision-making.
22
23
24

25 ³ *FBI, Secret Service Warn of Targeted Ransomware*, Law360 (Nov. 18, 2019),
26 <https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware> (last
27 visited June 4, 2024).

1 32. In 2016, the FTC updated its publication, Protecting Personal
2 Information: A Guide for Business, which established cyber-security guidelines for
3 businesses. The guidelines note that businesses should protect the personal customer
4 information that they keep; properly dispose of personal information that is no longer
5 needed; encrypt information stored on computer networks; understand their
6 network's vulnerabilities; and implement policies to correct any security problems.
7 The guidelines also recommend that businesses use an intrusion detection system to
8 expose a breach as soon as it occurs; monitor all incoming traffic for activity
9 indicating someone is attempting to hack the system; watch for large amounts of
10 data being transmitted from the system; and have a response plan ready in the event
11 of a breach.
12

13
14
15 33. The FTC further recommends that companies not maintain personally
16 identifiable information ("PII") longer than is needed for authorization of a
17 transaction; limit access to sensitive data; require complex passwords to be used on
18 networks; use industry-tested methods for security; monitor for suspicious activity
19 on the network; and verify that third-party service providers have implemented
20 reasonable security measures.
21

22
23 34. The FTC has brought enforcement actions against businesses for failing
24 to adequately and reasonably protect customer data, treating the failure to employ
25 reasonable and appropriate measures to protect against unauthorized access to
26
27

1 confidential consumer data as an unfair act or practice prohibited by Section 5 of the
2 Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from
3 these actions further clarify the measures businesses must take to meet their data
4 security obligations.

6 ***Defendant Failed to Comply with Industry Standards***

7 35. Defendant failed to properly implement basic data security practices.

8 36. Defendant was at all times fully aware of its obligation to protect the
9 Private Information of its clients. Defendant was also aware of the significant
10 repercussions that would result from its failure to do so.
11

12 37. Several best practices have been identified that at a minimum should be
13 implemented by consulting service providers like Defendant, including, but not
14 limited to educating all employees; strong passwords; multi-layer security, including
15 firewalls, anti-virus, and anti-malware software; encryption, making data unreadable
16 without a key; multi-factor authentication; backup data, and limiting which
17 employees can access sensitive data.
18

19 38. Other best cybersecurity practices that are standard in the consulting
20 industry include installing appropriate malware detection software; monitoring and
21 limiting the network ports; protecting web browsers and email management systems;
22 setting up network systems such as firewalls, switches, and routers; monitoring and
23 protection of physical security systems; protection against any possible
24
25
26
27

1 communication system; and training staff regarding critical points.

2 39. Defendant failed to meet the minimum standards of any of the
3 following frameworks: the NIST Cybersecurity Framework Version 1.1 (including
4 without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7,
5 PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7,
6 DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security
7 Controls (CIS CSC), which are all established standards in reasonable cybersecurity
8 readiness.
9

10
11 40. These foregoing frameworks are existing and applicable industry
12 standards in the consulting industry, and Defendant failed to comply with these
13 accepted standards, thereby opening the door to the cyber incident and causing the
14 Data Breach.
15
16

17 **DEFENDANT'S BREACH**

18 41. Defendant breached its obligations to Plaintiff and Class Members
19 and/or was otherwise negligent and reckless because it failed to properly maintain
20 and safeguard its computer systems and data. Defendant's negligent failure to protect
21 the confidentiality of Plaintiff and Class Members' Private Information includes, but
22 is not limited to, the following acts and/or omissions:
23
24

- 25 a. Failing to maintain an adequate data security system to reduce the
26 risk of data breaches and cyber-attacks;

- b. Failing to adequately protect client's Private Information;
- c. Failing to properly monitor its own data security systems for existing intrusions;
- d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;
- e. Failing to train its employees in the proper handling of emails containing Private Information and maintain adequate email security practices;
- f. Failing to adhere to industry standards for cybersecurity.

42. Defendant negligently and unlawfully failed to safeguard Plaintiff and Class Members' Private Information by allowing cyberthieves to access Defendant's computer network and systems which contained unsecured and unencrypted Private Information.

43. Accordingly, as outlined below, Plaintiff and Class Members now face a present and substantially increased risk of fraud and identity theft. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with Defendant.

Cyberattacks and Data Breaches Cause Disruption and Put Consumers at a Present and Substantially Increased Risk of Fraud and Identity Theft

44. Cyberattacks and data breaches at consulting service providers like Defendant are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

1 45. The United States Government Accountability Office released a report
2 in 2007 regarding data breaches (“GAO Report”) in which it noted that victims of
3 identity theft will face “substantial costs and time to repair the damage to their good
4 name and credit record.”⁴

6 46. That is because any victim of a data breach is exposed to serious
7 ramifications regardless of the nature of the data. Indeed, the reason criminals steal
8 personally identifiable information is to monetize it. They do this by selling the
9 spoils of their cyberattacks on the black market to identity thieves who desire to
10 extort and harass victims, take over victims’ identities in order to engage in illegal
11 transactions under the victims’ names. Because a person’s identity is akin to a
12 puzzle, the more accurate pieces of data an identity thief obtains about a person, the
13 easier it is for the thief to take on the victim’s identity, or otherwise harass or track
14 the victim. For example, armed with just a name and date of birth, a data thief can
15 utilize a hacking technique referred to as “social engineering” to obtain even more
16 information about a victim’s identity, such as a person’s login credentials or Social
17 Security number. Social engineering is a form of hacking whereby a data thief uses
18 previously acquired information to manipulate individuals into disclosing additional
19
20
21
22
23

24
25 ⁴ See U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are
26 Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is
27 Unknown (2007). Available at <https://www.gao.gov/new.items/d07737.pdf> (last accessed June 4,
28 2024).

1 confidential or personal information through means such as spam phone calls and
2 text messages or phishing emails.

3 47. The FTC recommends that identity theft victims take several steps to
4 protect their personal and financial information after a data breach, including
5 contacting one of the credit bureaus to place a fraud alert (consider an extended fraud
6 alert that lasts for 7 years if someone steals their identity), reviewing their credit
7 reports, contacting companies to remove fraudulent charges from their accounts,
8 placing a credit freeze on their credit, and correcting their credit reports.⁵
9

10 48. Identity thieves use stolen personal information such as Social Security
11 numbers for a variety of crimes, including credit card fraud, phone or utilities fraud,
12 and bank/finance fraud.
13

14 49. Identity thieves can also use Social Security numbers to obtain a
15 driver's license or official identification card in the victim's name but with the thief's
16 picture; use the victim's name and Social Security number to obtain government
17 benefits; or file a fraudulent tax return using the victim's information. In addition,
18 identity thieves may obtain a job using the victim's Social Security number, rent a
19 house or receive medical services in the victim's name, and may even give the
20 victim's personal information to police during an arrest resulting in an arrest warrant
21
22
23
24

25
26 ⁵ See *IdentityTheft.gov*, Federal Trade Commission, <https://www.identitytheft.gov/#/Steps> (last
27 accessed June 4, 2024).

1 being issued in the victim's name.

2 50. Moreover, theft of Private Information is also gravely serious. Private
3 Information is an extremely valuable property right.⁶
4

5 51. Its value is axiomatic, considering the value of "big data" in corporate
6 America and the fact that the consequences of cyber thefts include heavy prison
7 sentences. Even this obvious risk to reward analysis illustrates beyond doubt that
8 Private Information has considerable market value.
9

10 52. It must also be noted there may be a substantial time lag – measured in
11 years – between when harm occurs and when it is discovered, and also between when
12 Private Information and/or financial information is stolen and when it is used.
13

14 53. According to the U.S. Government Accountability Office, which
15 conducted a study regarding data breaches:
16

17 [L]aw enforcement officials told us that in some cases, stolen data may
18 be held for up to a year or more before being used to commit identity
19 theft. Further, once stolen data have been sold or posted on the Web,
20 fraudulent use of that information may continue for years. As a result,
21 studies that attempt to measure the harm resulting from data breaches
22 cannot necessarily rule out all future harm.

23 See GAO Report, at p. 29.

24 54. Private Information is such a valuable commodity to identity thieves

25 ⁶ See, e.g., John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable*
26 *Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4
27 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching
a level comparable to the value of traditional financial assets.") (citations omitted).

1 that once the information has been compromised, criminals often trade the
2 information on the “cyber black-market” for years.

3 55. There is a strong probability that entire batches of information stolen
4 from Defendant have been dumped on the black market and are yet to be dumped on
5 the black market, meaning Plaintiff and Class Members are at a present and
6 substantially increased risk of fraud and identity theft for many years into the future.
7

8 56. Thus, Plaintiff and Class Members must vigilantly monitor their
9 financial accounts for many years to come.
10

11 57. Sensitive Private Information can sell for as much as \$363 per record
12 according to the Infosec Institute.⁷ PII is particularly valuable because criminals can
13 use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of
14 that information and damage to victims may continue for years.
15
16

17 58. For example, the Social Security Administration has warned that
18 identity thieves can use an individual’s Social Security number to apply for
19 additional credit lines.⁸ Such fraud may go undetected until debt collection calls
20 commence months, or even years, later. Stolen Social Security Numbers also make
21
22
23

24 ⁷ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015),
25 <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/>
(last accessed June 4, 2024).

26 ⁸ *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1.
27 Available at <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last accessed June 4, 2024).

1 it possible for thieves to file fraudulent tax returns, file for unemployment benefits,
2 or apply for a job using a false identity. Each of these fraudulent activities is difficult
3 to detect. An individual may not know that his or her Social Security Number was
4 used to file for unemployment benefits until law enforcement notifies the
5 individual's employer of the suspected fraud. Fraudulent tax returns are typically
6 discovered only when an individual's authentic tax return is rejected.
7

8
9 59. Moreover, it is not an easy task to change or cancel a stolen Social
10 Security number.

11
12 60. The Private Information of individuals remains of high value to
13 criminals, as evidenced by the prices they will pay through the dark web. Numerous
14 sources cite dark web pricing for stolen identity credentials. For example, personal
15 information can be sold at a price ranging from \$40 to \$200, and bank details have
16 a price range of \$50 to \$200.⁹ Experian reports that a stolen credit or debit card
17 number can sell for \$5 to \$110 on the dark web.¹⁰ Criminals can also purchase access
18 to entire company data breaches from \$900 to \$4,500.¹¹
19
20

21
22 ⁹ *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct.
23 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last accessed June 4, 2024).

24 ¹⁰ *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec.
25 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last accessed June 4, 2024).

26 ¹¹ *In the Dark*, VPNOOverview, 2019, available at: <https://vpnooverview.com/privacy/anonymous-browsing/in-the-dark/> (last accessed June 4, 2024).
27

61. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.¹²

62. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."¹³

63. This data, as one would expect, demands a much higher price on the

¹² Social Security Administration, *Identity Theft and Your Social Security Number*, available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last accessed June 4, 2024).

¹³ Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft> (last accessed June 4, 2024).

1 black market. Martin Walter, senior director at cybersecurity firm RedSeal,
2 explained, “[c]ompared to credit card information, personally identifiable
3 information and Social Security Numbers are worth more than 10x on the black
4 market.”¹⁴

6 64. For this reason, Defendant knew or should have known about these
7 dangers and strengthened its data and email handling systems accordingly.
8 Defendant was put on notice of the substantial and foreseeable risk of harm from a
9 data breach, yet Defendant failed to properly prepare for that risk.

11 65. To date, Defendant has done nothing to provide Plaintiff and the Class
12 Members with relief for the damages they have suffered as a result of the Data
13 Breach.

15 66. Plaintiff’s and Class Members’ Private Information was compromised
16 in the Data Breach and is now in the hands of the cybercriminals who accessed
17 Defendant’s computer system. Upon information and belief, these cybercriminals
18 have published Plaintiff and Class Members’ Private Information to the internet.

20 67. Plaintiff and Class Members’ Private Information was compromised as
21 a direct and proximate result of the Data Breach.

24
25 ¹⁴ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card*
26 *Numbers*, Computer World (Feb. 6, 2015),
27 <https://www.networkworld.com/article/935334/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last accessed June 4, 2024).

Plaintiff Blake Mijangos's Experiences

68. Plaintiff received consulting services through Defendant.

69. As a condition to receiving the services, Plaintiff provided their Private Information to Defendant, with the expectation that the Private Information would be safeguarded against cyberattacks and foreseeable theft and not disclosed for unauthorized purposes.

70. Plaintiff is very careful about sharing his Private Information. Plaintiff has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Plaintiff stores any documents containing his sensitive PII in a safe and secure location or destroys the documents. Moreover, Plaintiff diligently chooses unique usernames and passwords for his various online accounts.

71. Plaintiff only allowed Defendant to maintain, store, and use his Private Information because he believed that Defendant would use basic security measures to protect his Private Information, such as requiring passwords and multi-factor authentication to access databases storing his Private Information. As a result, Plaintiff's Private Information was within the possession and control of Defendant at the time of the Data Breach.

72. Plaintiff received the Notice of Data Breach Letter dated May 31, 2024, from Defendant concerning the Data Breach. The Letter stated that the Plaintiff's full name, address, Social Security number, and date of birth were plausibly accessed

1 or stolen in the Data Breach.

2 73. Plaintiff suffered injury from a loss of privacy the moment that his
3 Private Information was accessed and exfiltrated by a third party without
4 authorization.
5

6 74. Recognizing the substantial risk Plaintiff faces, Defendant provided
7 Plaintiff a two-year subscription to a credit monitoring service.
8

9 75. Since learning of the Data Breach, Plaintiff has spent a significant
10 amount of time freezing his accounts, and reviewing bank statements, credit cards,
11 and credit monitoring applications for any fraud or suspicious activity.
12

13 76. The Data Breach has caused Plaintiff to suffer significant fear, anxiety,
14 and stress. Plaintiff has lost sleep thinking about all the ways the Sensitive
15 Information that was exposed can be used to commit fraud and identity theft.
16

17 77. The risk from the Data Breach has caused Plaintiff to spend significant
18 time dealing with issues related to the Data Breach, which includes time spent
19 verifying the legitimacy of the Notice of Data Breach, and self-monitoring his
20 accounts and credit reports to ensure no fraudulent activity has occurred. This time,
21 which has been lost forever and cannot be recaptured, was spent at Defendant's
22 direction.
23
24

25 78. Plaintiff plans on taking additional time-consuming, yet necessary,
26 steps to help mitigate the harm caused by the Data Breach, such as implementing
27

1 credit alerts.

2 ***Plaintiff's and Class Members' Injuries and Damages***

3 79. As a direct and proximate result of Defendant's conduct, Plaintiff and
4 Class Members have been placed at an imminent, immediate, and continuing
5 increased risk of harm from fraud and identity theft.
6

7 80. As a direct and proximate result of Defendant's conduct, Plaintiff and
8 Class Members have been forced to expend time dealing with the effects of the Data
9 Breach.
10

11 81. Plaintiff and Class Members face the present and substantially
12 increased risk of out-of-pocket fraud losses such as loans opened in their names,
13 medical services billed in their names, tax return fraud, utility bills opened in their
14 names, credit card fraud, and similar identity theft.
15
16

17 82. Plaintiff and Class Members face the present and substantially
18 increased risk of being targeted for future phishing, data intrusion, and other illegal
19 schemes based on their Private Information as potential fraudsters could use that
20 information to target such schemes more effectively to Plaintiff and Class Members.
21

22 83. Plaintiff and Class Members may also incur out-of-pocket costs for
23 protective measures such as credit monitoring fees, credit report fees, credit freeze
24 fees, and similar costs directly or indirectly related to the Data Breach.
25

26 84. Plaintiff and Class Members also suffered a loss of value of their
27

1 Private Information when it was acquired by cyber thieves in the Data Breach.
2 Numerous courts have recognized the propriety of loss of value damages in related
3 cases.
4

5 85. Plaintiff and Class Members were also damaged via benefit-of-the-
6 bargain damages. Plaintiff and Class Members overpaid for a service or product that
7 was intended to be accompanied by adequate data security but was not. Part of the
8 price Plaintiff and Class Members paid to Defendant was intended to be used by
9 Defendant to fund adequate security of Defendant's computer network and Plaintiff
10 and Class Members' Private Information. Thus, Plaintiff and the Class Members did
11 not get what they paid for and agreed to.
12
13

14 86. Plaintiff and Class Members have suffered or will suffer actual injury
15 as a direct result of the Data Breach. Many victims suffered ascertainable losses in
16 the form of out-of-pocket expenses and the value of their time reasonably incurred
17 to remedy or mitigate the effects of the Data Breach relating to:
18

- 19 a. Reviewing and monitoring sensitive accounts and finding fraudulent
20 insurance claims, loans, and/or government benefits claims;
21
- 22 b. Purchasing credit monitoring and identity theft prevention;
23
- 24 c. Placing "freezes" and "alerts" with reporting agencies;
25
- 26 d. Spending time on the phone with or at financial institutions,
27 healthcare providers, and/or government agencies to dispute
28 unauthorized and fraudulent activity in their name;

1 e. Contacting financial institutions and closing or modifying financial
2 accounts; and,

3 f. Closely reviewing and monitoring Social Security Number, bank
4 accounts, and credit reports for unauthorized activity for years to
5 come.

6 87. Moreover, Plaintiff and Class Members have an interest in ensuring that
7 their Private Information, which is believed to remain in the possession of
8 Defendant, is protected from further breaches by the implementation of security
9 measures and safeguards, including but not limited to, making sure that the storage
10 of data or documents containing Private Information is not accessible online and that
11 access to such data is password protected.
12

13 88. Further, because of Defendant's conduct, Plaintiff and Class Members
14 are forced to live with the anxiety that their Private Information may be disclosed to
15 the entire world, thereby subjecting them to embarrassment and depriving them of
16 any right to privacy whatsoever.
17
18

19 **CLASS ACTION ALLEGATIONS**

20 89. This action is properly maintainable as a class action. Plaintiff brings
21 this class action on behalf of himself, and all others similarly situated pursuant to
22 Fed. R. Civ. P. 23, for the following Class and Subclass defined as:
23

24 Nationwide Class: All individuals and entities residing in the United
25 States whose Private Information was compromised in the Data Breach
26 that occurred on, or around, February 5, 2024.
27

1 California Subclass: All individuals and entities residing or have
2 resided in California whose Private Information was compromised in
3 the Data Breach on, or around, February 5, 2024.

4 90. Excluded from the Classes are the following individuals and/or entities:
5 Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors,
6 and any entity in which Defendant has a controlling interest; all individuals who
7 make a timely election to be excluded from this proceeding using the correct protocol
8 for opting out; and all judges assigned to hear any aspect of this litigation, as well as
9 their immediate family members.
10

11 91. Plaintiff reserves the right to modify or amend the definition of the
12 proposed Classes before the Court determines whether certification is appropriate.
13

14 92. Numerosity: The members of the Classes are so numerous that joinder
15 of all members is impracticable, if not completely impossible. The Classes are
16 apparently identifiable within Defendant's records as the Notice Letter indicates.
17

18 93. Commonality and Predominance: Common questions of law and fact
19 exist as to all members of the Classes and predominate over any questions affecting
20 solely individual members of the Classes. Among the questions of law and fact
21 common to the Classes that predominate over questions which may affect individual
22 Class members, including the following:
23

- 24 a. Whether and to what extent Defendant had a duty to protect the
25 Private Information of Plaintiff and Class Members;
26

- b. Whether Defendant had a duty not to disclose the Private Information of Plaintiff and Class Members to unauthorized third parties;
- c. Whether Defendant had a duty not to use the Private Information of Plaintiff and Class Members for non-business purposes;
- d. Whether Defendant failed to adequately safeguard the Private Information of Plaintiff and Class Members;
- e. Whether and when Defendant actually learned of the Data Breach;
- f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their Private Information had been compromised;
- g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their Private Information had been compromised;
- h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the Private Information of Plaintiff and Class Members;
- k. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct;
- l. Whether Defendant was unjustly enriched by failing to properly protect Plaintiff and Class Members' Private Information;
- m. Whether Plaintiff and Class Members are entitled to restitution as a

1 result of Defendant's wrongful conduct; and

2 n. Whether Plaintiff and Class Members are entitled to injunctive relief
3 to redress the imminent and currently ongoing harm faced as a result
4 of the Data Breach.

5 94. Typicality: Plaintiff's claims are typical of those of the other members
6 of the Classes because Plaintiff, like every other member, was exposed to virtually
7 identical conduct and now suffers from the same violations of the law as other
8 members of the Classes
9

10 95. Policies Generally Applicable to the Classes: This class action is also
11 appropriate for certification because Defendant acted or refused to act on grounds
12 generally applicable to the Classes, thereby requiring the Court's imposition of
13 uniform relief to ensure compatible standards of conduct toward the Class Members
14 and making final injunctive relief appropriate with respect to the Nationwide Class
15 as a whole and to the California Subclass as a whole. Defendant's policies
16 challenged herein apply to and affect Class Members uniformly and Plaintiff's
17 challenge of these policies hinges on Defendant's conduct with respect to the Classes
18 each as a whole, not on facts or law applicable only to Plaintiff.
19
20
21

22 96. Adequacy: Plaintiff will fairly and adequately represent and protect the
23 interests of the Class Members in that he has no disabling conflicts of interest that
24 would be antagonistic to those of the other Class Members. Plaintiff seeks no relief
25 that is antagonistic or adverse to the Class Members and the infringement of the
26
27

rights and the damages they have suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

97. Superiority and Manageability: Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against a large corporation, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

98. Plaintiff and Class Members are ascertainable because Defendant's records will identify all victims of Defendant's Data Breach.

99. Plaintiff and Class Members are sufficiently numerous as to justify class action. Specifically, upon information and belief, the putative Class exceeds 27,000 individuals.

100. Plaintiff and Class Members have a well-defined community of interest

1 in pursuing relief from the harm that resulted from the Data Breach, including (1)
2 predominant common questions of law or fact; (2) a class representative with claims
3 or defenses typical of the class; and (3) a class representative who can adequately
4 represent the class.
5

6 101. The nature of this action and the nature of laws available to Plaintiff
7 and Class Members make the use of the class action device a particularly efficient
8 and appropriate procedure to afford relief to Plaintiff and Class Members for the
9 wrongs alleged because Defendant would necessarily gain an unconscionable
10 advantage since it would be able to exploit and overwhelm the limited resources of
11 each individual Class Member with superior financial and legal resources; the costs
12 of individual suits could unreasonably consume the amounts that would be
13 recovered; proof of a common course of conduct to which Plaintiff was exposed is
14 representative of that experienced by the Classes and will establish the right of each
15 Class Member to recover on the cause of action alleged; and individual actions
16 would create a risk of inconsistent results and would be unnecessary and duplicative
17 of this litigation.
18
19
20
21

22 102. The litigation of the claims brought herein is manageable. Defendant's
23 uniform conduct, the consistent provisions of the relevant laws, and the ascertainable
24 identities of Class Members demonstrates that there would be no significant
25 manageability problems with prosecuting this lawsuit as a class action.
26
27

1 103. Adequate notice can be given to Class Members directly using
2 information maintained in Defendant's records.

3 104. Unless a Class-wide injunction is issued, Defendant may continue in its
4 failure to properly secure the Private Information of Class Members, Defendant may
5 continue to refuse to provide proper notification to Class Members regarding the
6 Data Breach, and Defendant may continue to act unlawfully as set forth in this
7 Complaint.
8
9

10 **FIRST CAUSE OF ACTION**
11 **NEGLIGENCE**
12 **(On Behalf of Plaintiff and the Nationwide Class)**

13 105. Plaintiff and the Class repeat and reallege each and every allegation in
14 the Complaint as if fully set forth herein.

15 106. As a condition of receiving services from Defendant, Defendant's
16 current and former clients were obligated to provide Defendant with their Private
17 Information.
18

19 107. Plaintiff and the Class entrusted their Private Information to Defendant
20 on the premise and with the understanding that Defendant would use reasonable
21 measures to protect their Private Information and only make disclosures to third
22 parties that are authorized.
23
24

25 108. Defendant has full knowledge of the sensitivity of the Private
26 Information and the types of harm that Plaintiff and the Class could and would suffer
27

1 if the Private Information were wrongfully disclosed.

2 109. Defendant knew or reasonably should have known that the failure to
3 exercise due care in the collecting, storing, and using of the Private Information of
4 Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the
5 Class, even if the harm occurred through the criminal acts of a third party.
6

7 110. Defendant had a duty to exercise reasonable care in safeguarding,
8 securing, and protecting such information from being compromised, lost, stolen,
9 misused, and/or disclosed to unauthorized parties. This duty includes, among other
10 things, designing, maintaining, and testing Defendant's security protocols to ensure
11 that the Private Information of Plaintiff and the Class in Defendant's possession was
12 adequately secured and protected.
13

14 111. Defendant also had a duty to exercise appropriate clearinghouse
15 practices to remove former customers' Private Information that Defendant was no
16 longer required to retain pursuant to regulations or legitimate business purposes.
17

18 112. Defendant also had a duty to have procedures in place to detect and
19 prevent the improper access and misuse of the Private Information of Plaintiff and
20 the Class.
21

22 113. Defendant's duty to use reasonable security measures arose as a result
23 of the special relationship that existed between Defendant on the one hand and
24 Plaintiff and the Class on the other. That special relationship arose because Plaintiff
25
26
27

1 and the Class entrusted Defendant with their confidential Private Information, a
2 necessary part of receiving services from Defendant. The special relationship also
3 arose as a result of the nature of the relationship between Defendant and its clients.
4

5 114. Defendant was subject to an “independent duty,” untethered to any
6 contract between Defendant and Plaintiff or the Class.
7

8 115. A breach of security, unauthorized access, and resulting injury to
9 Plaintiff and the Class was reasonably foreseeable, particularly in light of
10 Defendant’s inadequate security practices.
11

12 116. Plaintiff and the Class were the foreseeable and probable victims of any
13 inadequate security practices and procedures. Defendant knew or should have
14 known of the inherent risks in collecting and storing the Private Information of
15 Plaintiff and the Class, the critical importance of providing adequate security of that
16 information, and the necessity for encrypting or redacting Private Information stored
17 on Defendant’s systems.
18

19 117. Defendant’s own conduct created a foreseeable risk of harm to Plaintiff
20 and the Class. Defendant’s misconduct included, but was not limited to, its failure
21 to take the steps and opportunities to prevent the Data Breach as set forth herein.
22 Defendant’s misconduct also included its decisions to not comply with industry
23 standards for the safekeeping of the Private Information of Plaintiff and the Class,
24 including basic encryption techniques freely available to Defendant.
25
26
27

1 118. Plaintiff and the Class had no ability to protect their Private Information
2 that was in, and possibly remains in, Defendant's possession.

3 119. Defendant was in a position to protect against the harm suffered by
4 Plaintiff and the Class as a result of the Data Breach.

5 120. Defendant had and continues to have a duty to adequately disclose that
6 the Private Information of Plaintiff and the Class within Defendant's possession
7 might have been compromised, how it was compromised, and precisely the types of
8 data that were compromised and when. Such notice was necessary to allow Plaintiff
9 and the Class to take steps to prevent, mitigate, and repair any identity theft and the
10 fraudulent use of their Private Information by third parties.

11 121. Defendant had a duty to employ proper procedures to prevent the
12 unauthorized dissemination of the Private Information of Plaintiff and the Class.

13 122. Defendant has admitted that the Private Information of Plaintiff and the
14 Class was accessed, exfiltrated, and published on the internet by cyber criminals.

15 123. Defendant, through its actions and/or omissions, unlawfully breached
16 its duties to Plaintiff and the Class by failing to implement industry protocols and
17 exercise reasonable care in protecting and safeguarding the Private Information of
18 Plaintiff and the Class during the time the Private Information was within
19 Defendant's possession or control.

20 124. Defendant improperly and inadequately safeguarded the Private
21 Information of Plaintiff and the Class.

1 Information of Plaintiff and the Class in deviation of standard industry rules,
2 regulations, and practices at the time of the Data Breach.

3 125. Defendant failed to heed industry warnings and alerts to provide
4 adequate safeguards to protect the Private Information of Plaintiff and the Class in
5 the face of increased risk of theft.
6

7 126. Defendant, through its actions and/or omissions, unlawfully breached
8 its duty to Plaintiff and the Class by failing to have appropriate procedures in place
9 to detect and prevent dissemination of its current and former patients' Private
10 Information.
11

12 127. Defendant, through its actions and/or omissions, unlawfully breached
13 its duty to adequately and timely disclose to Plaintiff and the Class the existence and
14 scope of the Data Breach.
15

16 128. But for Defendant's wrongful and negligent breach of duties owed to
17 Plaintiff and the Class, the Private Information of Plaintiff and the Class would not
18 have been compromised. There is a close causal connection between Defendant's
19 failure to implement security measures to protect the Private Information of Plaintiff
20 and the Class and the present harm, or risk of imminent harm, suffered by Plaintiff
21 and the Class. The Private Information of Plaintiff and Class Members was lost and
22 accessed as the proximate result of Defendant's failure to exercise reasonable care
23 in safeguarding such Private Information by adopting, implementing, and
24
25
26
27

1 maintaining appropriate security measures.

2 129. Defendant's violation of California and federal statutes also constitute
3 negligence *per se*. Specifically, as described herein, Defendant has violated
4 California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires
5 Defendant to undertake reasonable measures to safeguard the Private Information of
6 Plaintiff and the Class.
7

8 130. As a direct and proximate result of Defendant's negligence and
9 negligence *per se*, Plaintiff and Class Members have suffered and will suffer injury,
10 including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity
11 of how their Private Information is used; (iii) the compromise, publication, and/or
12 theft of their Private Information; (iv) out-of-pocket expenses associated with the
13 prevention, detection, and recovery from identity theft, tax fraud, and/or
14 unauthorized use of their Private Information; (v) lost opportunity costs associated
15 with effort expended and the loss of productivity addressing and attempting to
16 mitigate the actual present and future consequences of the Data Breach, including
17 but not limited to efforts spent researching how to prevent, detect, contest, and
18 recover from tax fraud and identity theft; (vi) costs associated with placing freezes
19 on credit reports; (vii) the continued risk to their Private Information, which remains
20 in Defendant's possession and is subject to further unauthorized disclosures so long
21 as Defendant fails to undertake appropriate and adequate measures to protect the
22
23
24
25
26
27

1 Private Information of Plaintiff and the Class; and (viii) costs in terms of time, effort,
2 and money that will be expended to prevent, detect, contest, and repair the impact of
3 the Private Information compromised as a result of the Data Breach for the remainder
4 of the lives of Plaintiff and the Class.

6 131. As a direct and proximate result of Defendant's negligence and
7 negligence *per se*, Plaintiff and the Class have suffered and will continue to suffer
8 other forms of injury and/or harm, including, but not limited to, anxiety, emotional
9 distress, loss of privacy, and other economic and non-economic losses.

11 132. Additionally, as a direct and proximate result of Defendant's
12 negligence and negligence *per se*, Plaintiff and Class Members have suffered and
13 will suffer the continued risks of exposure of their Private Information, which
14 remains in Defendant's possession and is subject to further unauthorized disclosures
15 so long as Defendant fails to undertake appropriate and adequate measures to protect
16 the Private Information in its continued possession.

19 133. Plaintiff and Class Members are therefore entitled to damages,
20 including restitution and unjust enrichment, declaratory and injunctive relief, and
21 attorneys' fees, costs, and expenses.

23 **SECOND CAUSE OF ACTION**
24 **INVASION OF PRIVACY**
25 **(On behalf of Plaintiff and the Nationwide Class)**

26 134. Plaintiff and the Class repeat and reallege each and every allegation in
27

1 the Complaint as if fully set forth herein.

2 135. Plaintiff and the Nationwide Class had a legitimate expectation of
3 privacy to their PII and were entitled to the protection of this information against
4 disclosure to unauthorized third parties.
5

6 136. Defendant owed a duty to its current and former clients, including
7 Plaintiff and the Nationwide Class, to keep their PII contained as a part thereof,
8 confidential.
9

10 137. Defendant failed to protect and actually or potentially released to
11 unknown and unauthorized third parties the PII of Plaintiff and the Nationwide
12 Class.
13

14 138. Defendant allowed unauthorized and unknown third parties to actually
15 or potentially access and examine the PII of Plaintiff and the Nationwide Class, by
16 way of Defendant's failure to protect the PII. The unauthorized release to, custody
17 of, and examination by unauthorized third parties of the PII of Plaintiff and the
18 Nationwide Class is highly offensive to a reasonable person.
19
20

21 139. The intrusion was into a place or thing, which was private and is entitled
22 to be private. Plaintiff and the Nationwide Class disclosed their PII to Defendant as
23 part of Plaintiff's and the Nationwide Class's relationships with Defendant, but
24 privately with an intention that the PII would be kept confidential and would be
25 protected from unauthorized disclosure.
26
27

140. Plaintiff and the Nationwide Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

141. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff and the Nationwide Class's interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

142. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and the Nationwide Class.

143. Moreover, as a result of the Data Breach, Plaintiff's Private Information is a private fact as a result of the Data Breach, Defendant publicly disclosed Plaintiff's and Class Members' private facts.

144. Plaintiff and Class Members' Private Information constitutes a private fact.

145. As a result of the Data Breach, Defendant publicly disclosed Plaintiff's and Class Members' Private Facts.

1 146. Defendant's public disclosure of Plaintiff's and Class Members'
2 Private Facts was offensive and objectionable to the reasonable person and is not of
3 a legitimate public concern.
4

5 147. As a proximate result of the above acts and omissions of Defendant,
6 the PII of Plaintiff and the Nationwide Class was accessed by third parties without
7 authorization, causing Plaintiff and the Nationwide Class to suffer damages.
8

9 148. Unless and until enjoined, and restrained by order of this Court,
10 Defendant's wrongful conduct will continue to cause great and irreparable injury to
11 Plaintiff and the Nationwide Class in that the PII maintained by Defendant can be
12 viewed, distributed, and used by unauthorized persons for years to come. Plaintiff
13 and the Nationwide Class have no adequate remedy at law for the injuries in that a
14 judgment for monetary damages will not end the invasion of privacy for Plaintiff
15 and the Nationwide Class.
16
17

18 **THIRD CAUSE OF ACTION**
19 **UNJUST ENRICHMENT**
20 **(On Behalf of Plaintiff and the Nationwide Class)**

21 149. Plaintiff and the Class repeat and reallege each and every allegation in
22 the Complaint as if fully set forth herein.
23

24 150. Defendant benefited from receiving Plaintiff and Class Members'
25 Private Information by its ability to retain and use that information for its own
26 benefit. Defendant understood this benefit.
27

1 151. Defendant also understood and appreciated that Plaintiff's and Class
2 Members' Private Information was private and confidential, and its value depended
3 upon Defendant maintaining the privacy and confidentiality of that information.
4

5 152. Plaintiff and Class Members conferred a monetary benefit upon
6 Defendant in the form of providing their Private Information to Defendant. In
7 connection thereto, Plaintiff and Class Members provided Private Information to
8 Defendant with the understanding that Defendant would pay for the administrative
9 costs of reasonable data privacy and security practices and procedures. Specifically,
10 Plaintiff and Class Members were required to provide their Private Information. In
11 exchange, Plaintiff and Class Members should have received adequate protection
12 and data security for such Private Information held by Defendant.
13
14

15 153. Defendant knew Plaintiff and Class Members conferred a benefit which
16 Defendant accepted. Defendant profited from these transactions and used the Private
17 Information of Plaintiff and Class Members for business purposes.
18

19 154. Defendant failed to provide reasonable security, safeguards, and
20 protections to the Private Information of Plaintiff and Class Members.
21

22 155. Under the principles of equity and good conscience, Defendant should
23 not be permitted to retain money belonging to Plaintiff and Class Members because
24 Defendant failed to implement appropriate data management and security measures
25 mandated by industry standards.
26
27

1 156. Defendant wrongfully accepted and retained these benefits to the
2 detriment of Plaintiff and Class Members.

3 157. Defendant's enrichment at the expense of Plaintiff and Class Members
4 is and was unjust.

5
6 158. As a result of Defendant's wrongful conduct, as alleged above, Plaintiff
7 and the Class Members are entitled to restitution and disgorgement of all profits,
8 benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs,
9 and interest thereon.
10

11 **FOURTH CAUSE OF ACTION**
12 **BREACH OF IMPLIED CONTRACT**
13 **(On behalf of Plaintiff and the Nationwide Class)**

14 159. Plaintiff and Class Members repeat and reallege each and every
15 allegation in the Complaint as if fully set forth herein.
16

17 160. Plaintiff and the Class Members delivered their Private Information to
18 Defendant as part of the process of obtaining services provided by Defendant.

19 161. Plaintiff and Class Members entered into implied contracts with
20 Defendant under which Defendant agreed to safeguard and protect such information
21 and to timely and accurately notify Plaintiff and Class Members if and when their
22 data had been breached and compromised. Each such contractual relationship
23 imposed on Defendant an implied covenant of good faith and fair dealing by which
24 Defendant was required to perform its obligations and manage Plaintiff and Class
25
26
27

Members' data in a manner which comported with the reasonable expectations of privacy and protection attendant to entrusting such data to Defendant.

162. In providing their Private Information, Plaintiff and Class Members entered into an implied contract with Defendant whereby Defendant, in receiving such data, became obligated to reasonably safeguard Plaintiff's and the other Class Members' Private Information.

163. In delivering their Private Information to Defendant, Plaintiff and Class Members intended and understood that Defendant would adequately safeguard that data.

164. Plaintiff and the Class Members would not have entrusted their Private Information to Defendant in the absence of such an implied contract.

165. Defendant accepted possession of Plaintiff's and Class Members' personal data for the purpose of providing medical services to Plaintiff and Class Members.

166. Had Defendant disclosed to Plaintiff and Class Members that Defendant did not have adequate computer systems and security practices to secure their Private Information, Plaintiff and Class Members would not have provided their Private Information to Defendant.

167. Defendant recognized that its current and former client's Private Information is highly sensitive and must be protected, and that this protection was

1 of material importance as part of the bargain to Plaintiff and Class Members.

2 168. Plaintiff and Class Members fully performed their obligations under the
3 implied contracts with Defendant.
4

5 169. Defendant breached the implied contract with Plaintiff and Class
6 Members by failing to take reasonable measures to safeguard their data.
7

8 170. Defendant breached the implied contract with Plaintiff and Class
9 Members by failing to promptly notify them of the access to and exfiltration of their
10 Private Information.
11

12 171. As a direct and proximate result of the breach of the contractual duties,
13 Plaintiff and Class Members have suffered actual, concrete, and imminent injuries.
14 The injuries suffered by Plaintiff and the Class Members include: (a) the invasion of
15 privacy; (b) the compromise, disclosure, theft, and unauthorized use of Plaintiff's
16 and Class Members' Private Information; (c) economic costs associated with the
17 time spent to detect and prevent identity theft, including loss of productivity; (d)
18 monetary costs associated with the detection and prevention of identity theft; (e)
19 economic costs, including time and money, related to incidents of actual identity
20 theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing
21 related to the theft and compromise of their Private Information; (g) the diminution
22 in the value of the services bargained for as Plaintiff and Class Members were
23 deprived of the data protection and security that Defendant promised when Plaintiff
24
25
26
27

1 and the proposed class entrusted Defendant with their Private Information; and (h)
2 the continued and substantial risk to Plaintiff and Class Members' Private
3 Information, which remains in the Defendant's possession with inadequate measures
4 to protect Plaintiff's and Class Members' Private Information.
5

6 **FIFTH CAUSE OF ACTION**
7 **VIOLATION OF CALIFORNIA'S**
8 **UNFAIR COMPETITION LAW ("UCL")**
9 **UNLAWFUL BUSINESS PRACTICE**
10 **(CAL BUS. & PROF. CODE § 17200, *ET SEQ.*)**
11 **(On Behalf of Plaintiff and the Nationwide Class or, alternatively,**
12 **the California Subclass)**

13 172. Plaintiff and the Class repeat and reallege each and every allegation in
14 the Complaint as if fully set forth herein.

15 173. By reason of the conduct alleged herein, Defendant engaged in
16 unlawful "business practices" within the meaning of the UCL.

17 174. Defendant stored client data of Plaintiff and the Class Members in its
18 computer systems. Defendant falsely represented to Plaintiff and the Class Members
19 that their Private Information was secure and would remain private.
20

21 175. Defendant knew or should have known it did not employ reasonable,
22 industry standard, and appropriate security measures that would have kept Plaintiff
23 and the Class Member's Private Information secure and prevented the loss or misuse
24 of that Private Information.
25

26 176. Even without these misrepresentations, Plaintiff and Class Members
27

1 were entitled to assume, and did assume Defendant would take appropriate measures
2 to keep their Private Information safe. Defendant did not disclose at any time that
3 Plaintiff Private Information was vulnerable to hackers because Defendant's data
4 security measures were inadequate and outdated, and Defendant was the only entity
5 in possession of that material information, which it had a duty to disclose. Defendant
6 violated the UCL by misrepresenting, both by affirmative conduct and by omission,
7 the safety of its computer systems, specifically the security thereof, and its ability to
8 safely store Plaintiff and Class Members' Private Information. Defendant also
9 violated the UCL by failing to implement reasonable and appropriate security
10 measures or follow industry standards for data security, failing to comply with its
11 own posted privacy policies, and by failing to immediately notify Plaintiff and Class
12 Members of the Data Breach. If Defendant had complied with these legal
13 requirements, Plaintiff and Class Members would not have suffered the damages
14 related to the Data Breach, and consequently from, Defendant's failure to timely
15 notify Plaintiff and the Class Members of the Data Breach.
16
17
18
19
20

21 177. Plaintiff and Class Members suffered injury in fact and lost money or
22 property as the result of Defendant's unlawful business practices. In particular,
23 Plaintiff and Class Members have suffered from improper or fraudulent charges to
24 their credit/debit card accounts; and other similar harm, all as a result of the Data
25 Breach. In addition, their Private Information was taken and is in the hands of those
26
27

1 who will use it for their own advantage, or is being sold for value, making it clear
2 that the hacked information is of tangible value. Plaintiff and Class Members have
3 also suffered consequential out of pocket losses for procuring credit freeze or
4 protection services, identity theft monitoring, and other expenses relating to identity
5 theft losses or protective measures.
6

7 178. As a result of Defendant's unlawful business practices, violations of
8 the UCL, Plaintiff and the Class Members are entitled to injunctive relief.
9

10 **SIXTH CAUSE OF ACTION**
11 **VIOLATION OF CALIFORNIA'S UNFAIR**
12 **COMPETITION LAW ("UCL")**
13 **UNFAIR BUSINESS PRACTICE (CAL BUS. & PROF.**
14 **CODE § 17200, *ET SEQ.*)**
15 **(On behalf of Plaintiff and the Nationwide Class or, alternatively, the**
16 **California Subclass)**

17 179. Plaintiff and Class Members repeat and reallege each and every
18 allegation in the Complaint as if fully set forth herein.
19

20 180. By reason of the conduct alleged herein, Defendant engaged in unfair
21 "business practices" within the meaning of the UCL.
22

23 181. Defendant stored Plaintiff and Class Members' Private Information in
24 its electronic and consumer information databases. Defendant represented to
25 Plaintiff and Class Members that their Private Information was secure, and that
26 Plaintiff and the Class Members' Private Information would remain private.
27 Defendant engaged in unfair acts and business practices by representing that it had
28

1 secure computer systems when it did not.

2 182. Even without these misrepresentations, Plaintiff and the Class
3 Members were entitled to, and did, assume Defendant would take appropriate
4 measures to keep their Private Information safe. Defendant did not disclose at any
5 time that Plaintiff and Class Members' Private Information was vulnerable to
6 hackers because Defendant's data security measures were inadequate and outdated,
7 and Defendant was the only entity in possession of that material information, which
8 it had a duty to disclose.
9

10
11 183. Defendant knew or should have known it did not employ reasonable
12 measures that would have kept Plaintiff and the Class Members' Private Information
13 secure and prevented the loss or misuse of Plaintiff and the Class Members' Private
14 Information.
15

16
17 184. Defendant violated the UCL by misrepresenting, both by affirmative
18 conduct and by omission, the security of its systems and services, and its ability to
19 safely store Plaintiff and the Class Members' Private Information. Defendant also
20 violated the UCL by failing to implement and maintain reasonable security
21 procedures and practices appropriate to protect Private Information, and by failing
22 to immediately notify Plaintiff and the Class Members of the Data Breach.
23

24
25 185. Defendant also violated its commitment to maintain the confidentiality
26 and security of Plaintiff's and the Class Members' Private Information and failed to
27

1 comply with its own policies and applicable laws, regulations, and industry
2 standards relating to data security.

3 186. **Defendant engaged in unfair business practices under the**
4 **“balancing test.”** The harm caused by Defendant’s actions and omissions, as
5 described in detail above, greatly outweigh any perceived utility. Indeed,
6 Defendant’s failure to follow basic data security protocols and misrepresentations to
7 Plaintiff and Class Members about Defendant’s data security cannot be said to have
8 had any utility at all. All these actions and omissions were clearly injurious to
9 Plaintiff and the Class Members, directly causing the harms alleged below.
10
11

12 187. **Defendant engaged in unfair business practices under the**
13 **“tethering test.”** Defendant’s actions and omissions, as described in detail above,
14 violated fundamental public policies expressed by the California Legislature. *See,*
15 *e.g.*, Cal. Civ. Code § 1798.1 (“The Legislature declares that ... all individuals have
16 a right of privacy in information pertaining to them.... The increasing use of
17 computers ... has greatly magnified the potential risk to individual privacy that can
18 occur from the maintenance of personal information.”); Cal. Civ. Code §
19 1798.81.5(a) (“It is the intent of the Legislature to ensure that personal information
20 about California residents is protected.”); Cal. Bus. & Prof. Code § 22578 (“It is the
21 intent of the Legislature that this chapter [including the Online Privacy Protection
22 Act] is a matter of statewide concern.”) Defendant’s acts and omissions, and the
23
24
25
26
27

injuries caused by them, are thus “comparable to or the same as a violation of the law ...” *Cel-Tech Communications, Inc. v. Los Angeles Cellular Telephone Co.* (1999) 20 Cal. 4th 163, 187.

188. **Defendant engaged in unfair business practices under the “FTC test.”** The harm caused by Defendant’s actions and omissions, as described in detail above, is substantial in that it affects tens of thousands of Class Members and has caused those persons to suffer actual harms. Such harms include a substantial risk of identity theft, disclosure of Plaintiff’s and the Class Members’ Private Information to third parties without their consent, diminution in value of their Customer Data, consequential out of pocket losses for procuring credit freeze or protection services, identity theft monitoring, and other expenses relating to identity theft losses or protective measures. This harm continues given the fact that Plaintiffs’ and the Class Members’ Private Information remains in Defendant’s possession, without adequate protection, and is also in the hands of those who obtained it without their consent. Defendant’s actions and omissions violated, *inter alia*, Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45. *See, e.g., F.T.C. v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602, 613 (D.N.J. 2014), *aff’d*, 799 F.3d 236 (3d Cir. 2015); *In re LabMD, Inc.*, FTC Docket No. 9357, FTC File No. 102-3099 (July 28, 2016) (failure to employ reasonable and appropriate measures to secure personal information collected violated § 5(a) of FTC Act); *In re BJ’s Wholesale Club, Inc.*,

1 FTC Docket No. C-4148, FTC File No. 042-3160 (Sept. 20, 2005) (same); *In re*
2 *CardSystems Solutions, Inc.*, FTC Docket No. C-4168, FTC File No. 052-3148
3 (Sept. 5, 2006) (same); *see also United States v. ChoicePoint, Inc.*, Civil Action No.
4 1:06-cv-0198-JTC (N.D. Ga. Oct. 14, 2009) (“failure to establish and implement,
5 and thereafter maintain, a comprehensive information security program that is
6 reasonably designed to protect the security, confidentiality, and integrity of personal
7 information collected from or about consumers” violates § 5(a) of FTC Act); 15
8 U.S.C. § 45(n) (defining “unfair acts or practices” as those that “cause[] or[are]
9 likely to cause substantial injury to consumers which [are] not reasonably avoidable
10 by consumers themselves and not outweighed by countervailing benefits to
11 consumers or to competition.”).

12
13
14
15 189. Plaintiff and the Class Members suffered injury in fact and lost money
16 or property as the result of Defendant’s unfair business practices. In particular,
17 Plaintiff and the Class Members have suffered from improper or fraudulent charges
18 to their credit/debit card accounts; and other similar harm, all as a result of the Data
19 Breach. In addition, their Private Information was taken and is in the hands of those
20 who will use it for their own advantage, or is being sold for value, making it clear
21 that the hacked information is of tangible value. Plaintiff and the Class Members
22 have also suffered consequential out of pocket losses for procuring credit freeze or
23 protection services, identity theft monitoring, and other expenses relating to identity
24
25
26
27

1 theft losses or protective measures.

2 190. As a result of Defendant's unfair business practices, violations of the
3 UCL, Plaintiff and the Class Members are entitled to injunctive relief.
4

5 **SEVENTH CAUSE OF ACTION**
6 **BREACH OF CALIFORNIA SECURITY NOTIFICATION LAWS**
7 **(On behalf of Plaintiff and the Nationwide Class or, alternatively, the**
8 **California Subclass)**

9 191. Plaintiff and Class Members repeat and reallege each and every
10 allegation in the Complaint as if fully set forth herein.

11 192. Pursuant to Civil Code § 1798.82(a), "A person or business that
12 conducts business in California, and that owns or licenses computerized data that
13 includes personal information, shall disclose a breach of the security of the system
14 following discovery or notification of the breach in the security of the data to a
15 resident of California (1) whose unencrypted personal information was, or is
16 reasonably believed to have been, acquired by an unauthorized person, or, (2) whose
17 encrypted personal information was, or is reasonably believed to have been, acquired
18 by an unauthorized person and the encryption key or security credential was, or is
19 reasonably believed to have been, acquired by an unauthorized person and the person
20 or business that owns or licenses the encrypted information has a reasonable belief
21 that the encryption key or security credential could render that personal information
22 readable or usable. The disclosure shall be made in the most expedient time possible
23
24
25
26
27

1 and without unreasonable delay, consistent with the legitimate needs of law
2 enforcement, as provided in subdivision (c), or any measures necessary to determine
3 the scope of the breach and restore the reasonable integrity of the data system.” Prior
4 to passage of such statute, the California State Assembly cited an incident where
5 authorities knew of the breach in security for 21 days “before state workers were
6 told” as an example of “late notice.”
7

8
9 193. Civil Code § 1798.82 further provides, “(h) For purposes of this section,
10 ‘personal information’ means an individual’s first name or first initial and last name
11 in combination with any one or more of the following data elements, when either the
12 name or the data elements are not encrypted: (1) Social security number. (2) Driver’s
13 license number or California Identification Cardnumber. (3) Account number, credit
14 or debit card number, in combination with any required security code, access code,
15 or password that would permit access to an individual’s financial account. (4)
16 Medical information. (5) Health insurance information. (i) (2) For purposes of
17 this section.
18
19
20

21 194. Defendant conducts business in California and owns or licenses
22 computerized data which includes the personal information, within the meaning of
23 Civil Code § 1798.82(h), of Plaintiff and the Class.
24

25 195. Based upon Defendant’s Notice of Data Incident Letter, Defendant was
26 aware that Plaintiff and the Class Members’ unencrypted personal information was,
27

1 or is reasonably believed to have been, acquired by an unauthorized person no later
2 than April 12, 2024, but did not begin to mail notification letters to Plaintiff and the
3 Class until May 31, 2024. Thus, Defendant waited at least 49 days before *beginning*
4 to inform Plaintiff and the Class of this incident and the subsequent threat to Plaintiff
5 and the Class Members' unencrypted personal information. As a result, Defendant
6 did not disclose to Plaintiff and the Class Members that their unencrypted personal
7 information was, or was reasonably believed to have been, acquired by an
8 unauthorized person, in the most expedient time possible and without reasonable
9 delay in violation of Civil Code § 1798.82(a). Given the example of the Legislature
10 finding that a delay of 21 days to be "late notice" under the statute, Defendant's
11 delay of 49 days before *beginning* to inform Plaintiff and Class Members that their
12 personal information was, or was reasonably believed to have been, acquired by an
13 unauthorized person by mailing Defendant's Notice of Data Security Incident Letter
14 to Plaintiff and Class Members is a presumptively unreasonable notice in violation
15 of Civil Code § 1798.82(a).
16
17
18
19
20

21 196. Upon information and belief, Plaintiff believes and alleges that no law
22 enforcement agency has notified Defendants that the notification would impede a
23 criminal investigation justifying Defendant's decision to wait 49 days *before*
24 *beginning to mail* notification letters to Plaintiff and Class Members *after* they knew
25 that Plaintiff and Class Members unencrypted personal information on Defendant's
26
27

1 network server was, or was reasonably believed to have been, acquired by an
2 unauthorized person. Upon information and belief, Plaintiff believes and alleges that
3 there were no measures taken by Defendant to determine the scope of the breach or
4 to restore the reasonable integrity of the data system, which justifies Defendant's
5 decision to wait 49 days *before beginning to mail* notification letters to Plaintiff and
6 Class Members. Moreover, Form I-9's Notice of Data Security Incident Letter
7 mailed to Plaintiff and Class *failed* to state whether notification was delayed as a
8 result of a law enforcement investigation, in violation of Civil Code §
9 1798.82(d)(2)(D).
10
11
12

13 197. Plaintiff and Class Members have been injured by fact that Defendants
14 did not disclose to them that their unencrypted personal information was, or was
15 reasonably believed to have been, acquired by an unauthorized person in the most
16 expedient time possible and without reasonable delay in violation of Civil Code §
17 1798.82(a). Defendant's delays in informing required by Civil Code § 1798.82(a)
18 and providing all of the information required by Civil Code § 1798.82(d) to Plaintiff
19 and Class Members that their unencrypted personal information was, or was
20 reasonably believed to have been, acquired by an unauthorized person, have
21 prevented Plaintiff and Class Members from taking steps in the most expedient time
22 possible to protect their unencrypted personal information from unauthorized use
23 and/or identify theft.
24
25
26
27

1 198. As a direct and proximate result of Defendant's and/or its employees'
2 above-described conduct in violation of Civil Code § 1798.82(a), Plaintiff and Class
3 Members seek damages suffered, according to proof, pursuant to Civil Code §
4 1798.84(b), and injunctive relief pursuant to Civil Code § 1798.84(e), from the
5 Defendant.
6

7
8 **PRAYER FOR RELIEF**

9 **WHEREFORE**, Plaintiff, on behalf of himself and Class Members, request
10 judgment against Defendant and that the Court grant the following:

- 11 A. For an order certifying the Class, as defined herein, and appointing
12 Plaintiff and their Counsel to represent each such Class;
- 13 B. For equitable relief enjoining Defendant from engaging in the wrongful
14 conduct complained of herein pertaining to the misuse and/or
15 disclosure of the Private Information of Plaintiff and Class Members,
16 and from refusing to issue prompt, complete, and accurate disclosures
17 to Plaintiff and Class Members;
- 18 C. For injunctive relief requested by Plaintiff, including, but not limited
19 to, injunctive and other equitable relief as is necessary to protect the
20 interests of Plaintiff and Class Members, including but not limited to
21 an order:
- 22 i. prohibiting Defendant from engaging in the wrongful and unlawful
23 acts described herein;
- 24 ii. requiring Defendant to protect, including through encryption, all
25 data collected through the course of its business in accordance with
26 all applicable regulations, industry standards, and federal, state or
27 local laws;
- 28 iii. requiring Defendant to delete, destroy, and purge the personal
identifying information of Plaintiff and Class Members unless

1 Defendant can provide to the Court reasonable justification for the
2 retention and use of such information when weighed against the
3 privacy interests of Plaintiff and Class Members;

4 iv. requiring Defendant to implement and maintain a comprehensive
5 Information Security Program designed to protect the
6 confidentiality and integrity of the Private Information of Plaintiff
7 and Class Members;

8 v. prohibiting Defendant from maintaining the Private Information of
9 Plaintiff and Class Members on a cloud-based database;

10 vi. requiring Defendant to engage independent third-party security
11 auditors/penetration testers as well as internal security personnel to
12 conduct testing, including simulated attacks, penetration tests, and
13 audits on Defendant's systems on a periodic basis, and ordering
14 Defendant to promptly correct any problems or issues detected by
15 such third-party security auditors;

16 vii. requiring Defendant to engage independent third-party security
17 auditors and internal personnel to run automated security
18 monitoring;

19 viii. requiring Defendant to audit, test, and train its security personnel
20 regarding any new or modified procedures;

21 ix. requiring Defendant to segment data by, among other things,
22 creating firewalls and access controls so that if one area of
23 Defendant's network is compromised, hackers cannot gain access to
24 other portions of Defendant's systems;

25 x. requiring Defendant to conduct regular database scanning and
26 securing checks;

27 xi. requiring Defendant to establish an information security training
28 program that includes at least annual information security training
for all employees, with additional training to be provided as
appropriate based upon the employees' respective responsibilities
with handling personal identifying information, as well as protecting

1 the personal identifying information of Plaintiff and Class
2 Members;

3 xii. requiring Defendant to routinely and continually conduct internal
4 training and education, and on an annual basis to inform internal
5 security personnel how to identify and contain a breach when it
6 occurs and what to do in response to a breach;

7 xiii. requiring Defendant to implement a system of tests to assess its
8 employees' knowledge of the education programs discussed in the
9 preceding subparagraphs, as well as randomly and periodically
10 testing employees' compliance with Defendant's policies,
11 programs, and systems for protecting personal identifying
12 information;

13 xiv. requiring Defendant to implement, maintain, regularly review, and
14 revise as necessary a threat management program designed to
15 appropriately monitor Defendant's information networks for threats,
16 both internal and external, and assess whether monitoring tools are
17 appropriately configured, tested, and updated;

18 xv. requiring Defendant to meaningfully educate all Class Members
19 about the threats that they face as a result of the loss of their
20 confidential Private Information to third parties, as well as the steps
21 affected individuals must take to protect themselves;

22 xvi. requiring Defendant to implement logging and monitoring programs
23 sufficient to track traffic to and from Defendant's servers; and for a
24 period of 10 years, appointing a qualified and independent third-
25 party assessor to conduct a SOC 2 Type 2 attestation on an annual
26 basis to evaluate Defendant's compliance with the terms of the
27 Court's final judgment, to provide such report to the Court and to
28 counsel for the class, and to report any deficiencies with compliance
of the Court's final judgment;

D. For an award of damages, including actual, statutory, nominal, and
consequential damages, as allowed by law in an amount to be
determined;

- 1 E. For an award of attorneys' fees, costs, and litigation expenses, as
2 allowed by law;
- 3 F. For prejudgment and/or post-judgment interest on all amounts awarded;
4 and
- 5 G. Such other and further relief as this Court may deem just and proper.

6 **DEMAND FOR JURY TRIAL**

7 Plaintiff hereby demands that this matter be tried before a jury.

8
9 DATED: June 5, 2024

Respectfully Submitted,

10 /s/ Bryan L. Bleichner

11 **CHESTNUT CAMBRONNE PA**

12 Bryan L. Bleichner (CAL BAR # 220340)

13 100 Washington Avenue South, Suite 1700

14 Minneapolis, MN 55401

15 Phone: (612) 339-7300

16 Email: *bbleichner@chesnutcambronne.com*